UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,231	07/31/2001	Brian J. Matt	NA01-00101	6007

28875 7590 05/13/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/921,231	MATT, BRIAN J.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20050408*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 28 January 2005. Claims 1, 2, 11, and 18-21 have been amended. No claims have been added or canceled. Claims 1-21 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 28 January 2005 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 1-21 under 35 U.S.C. 103(a) as unpatentable over Menezes et al, *Handbook of Applied Cryptography*, and specifically in reference to independent Claim 1, Applicant argues that any disclosure in Menezes of message authentication codes (MACs) and identity-based keying fails to meet the claim language regarding the MAC and the second node key in Claim 1. However, it appears that a limitation that the Applicant alleges is not met simply refers to the addition of a message authentication code to the second message of the message authentication code. The Examiner believes that the protocol disclosed in Menezes already discloses such a second message (page 503, protocol 12.26, message 1), and that one of ordinary skill would further be motivated to include a MAC in such a message to provide data origin authentication and data integrity, as stated in the previous Office action (see Menezes, page 361, definition 9.77). Applicant further points to the limitation of verifying the

message authentication code as not met; however, the Examiner believes that once the MAC has been included in a message, it must be verified to provide the aforementioned benefits. Additionally, it appears that a second limitation that Applicant alleges is not met simply refers to the generation of the second node key based on the second node identifier; the Examiner believes that since the protocol disclosed in Menezes already discloses the use and distribution of keys, one of ordinary skill in the art would further be motivated to include the use of key generation based on an identifier to prevent forgery and impersonation, as stated in the previous Office action (see Menezes, page 561, section 13.4.3).

In response to applicant's arguments that it would "be unobvious to modify Menezes to meet applicant's claim limitations noted above, especially in view of the numerous advantages provided by such claim limitations" (page 13 of the present response), the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985).

Applicant's arguments regarding the new limitation of the independent claims, namely "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar", fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-21 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, independent claims 1, 18, and 20 have been amended to recite the limitation "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar". This limitation has not been described anywhere in Applicant's specification. All other claims are rejected due to their dependence on a rejected base claim.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 18, and 20 each recite the limitation "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar". This limitation is generally unclear. It is not clear how something can be capable of being avoided at least in part; it would either be capable of being avoided or not. This renders the claims indefinite.

Claims 2, 11, 19, and 21 each recite the limitation "verifying the hash value"; however, it is not clear whether the verifications take place at the first node, the second node, or the key distribution center. This renders the claims indefinite.

All other claims not referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al, *Handbook of Applied Cryptography*.

In reference to Claim 1, Menezes discloses the Needham-Schroeder key distribution protocol, a method that includes requesting establishing a cryptographic key between a first node and a second node, sending a message from the second node to a key distribution center that includes identifiers for the nodes (page 503, protocol 12.26, message 1), generating a cryptographic key at the key distribution center, and communicating the cryptographic key to the first and second nodes (page 503, protocol 12.26, message 2). Although the protocol does not explicitly disclose the use of message authentication codes, or recreating a second node key previously created using the second node identifier and a secret key of the key distribution center, Menezes discloses both MACs (see page 361, below definition 9.77) and identity-based keying (page 561, section 13.4.3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the key distribution protocol by including the use of a MAC, in order to provide data origin authentication and data integrity (see Menezes, page 361, definition 9.77) and by including identity-based keying, in order to prevent forgery and impersonation (see Menezes, page 561, section 13.4.3).

In reference to Claim 2, Menezes further discloses communicating the cryptographic key to the nodes by encrypting the cryptographic key using the second node key to form a first encrypted key, encrypting the cryptographic key using the first node key to form a second encrypted key, sending a message from the key distribution center to the second node that includes the first and second encrypted keys (page 503. protocol 12.26, message 2), decrypting the first encrypted key at the second node to

recover the cryptographic key, sending the second encrypted key and a key confirmation value to the first node (page 503, protocol 12.26, messages 3 and 5), decrypting the second encrypted key at the first node to recover the cryptographic key, establishing at the first node that the second node has the cryptographic key using the key confirmation value, and sending a message to the second node from the first node so the second node can establish that the first node has the cryptographic key (page 503, protocol 12.26, message 4). Although the protocol does not explicitly disclose recreating a first node key previously created using the first node identifier and the secret key, Menezes discloses identity-based keying (page 561, section 13.4.3). Further, although the protocol does not explicitly disclose the use of a hash value in the messages for verification, Menezes discloses that hash values can be used for verification of data (see, for example, page 322, first full paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the key distribution protocol by including the use of a hash, in order to provide data integrity (see Menezes, pages 321-322, section 9.1).

In reference to Claims 3 and 4, Menezes further discloses that the messages include the node identifiers and a nonce (page 503, protocol 12.26, message 1).

In reference to Claim 5, Menezes further discloses verifying the message authentication code by creating a test MAC to compare with the original MAC (pages 321-322, section 9.1).

In reference to Claim 6, 8, and 11, Menezes further discloses verifying the hash value by creating a hash value and creating test hash values to compare with the original hash value (page 322, first full paragraph).

In reference to Claim 7, Menezes further discloses that a message includes the node identifiers and the encrypted keys (page 503, protocol 12.26, message 2).

In reference to Claims 9 and 10, Menezes further discloses that a message includes identifiers, a nonce, and a confirmation value that includes an encrypted nonce (page 503, protocol 12.26, message 5).

In reference to Claims 12 and 15, Menezes discloses that each node confirms that the other has the cryptographic key by verifying nonces (page 503, protocol 12.26, messages 4 and 5).

In reference to Claims 13 and 14, Menezes further discloses that a message includes identifiers and an encrypted confirmation value (page 503, protocol 12.26, message 4).

In reference to Claims 16 and 17, Menezes discloses identity-based keying (page 561, section 13.4.3) and that the node keys are installed in the node prior to deployment (page 503, protocol 12.26, "One-time setup").

Claims 18 and 19 are directed to software implementations of the methods of Claims 1 and 2, and are rejected by a similar rationale.

Similarly, Claims 20 and 21 are directed to an apparatus corresponding substantially to the methods of Claims 1 and 2, and are rejected by a similar rationale.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER